



Standards and Implementation Specifications

(Required vs. Addressable)

HS-IP-3

November 2003

H I P A A S e c u r i t y C o m p l i a n c e



**TMA Privacy
Office**

**5111
Leesburg Pike
Suite 810
Falls Church
VA 22041**

How is the Security Rule structured?

The safeguards required by HIPAA's Security Rule are divided into three categories; administrative, physical and technical. The three safeguard categories are further divided into standards that describe what each covered entity must do to meet the objectives of the Security Rule. In some cases, the standard itself contains enough information to describe implementation requirements, so there is no separate specification. Other standards have associated "implementation specifications" that expand on or explain what is required by the standard.

How does a covered entity decide what to do?

All standards are required and must be met. Implementation specifications are either "required" or "addressable". A required implementation specification means just that; it must be done. An addressable implementation specification must be "assessed" and "reasonable and appropriate" action taken. Each covered entity must base their decision as to what is "reasonable and appropriate" on its risk analysis, its mitigation strategy for those risks, security measures already in place, and the costs of alternatives. Once that has been done the following decision steps apply. If an addressable implementation specification is determined to be:

- reasonable and appropriate given the circumstances of the covered entity, it must be implemented;
- unreasonable or inappropriate, but the standard cannot be met without it, then an alternative measure that accomplishes the same end must be put in place;
- unreasonable or inappropriate, or simply not applicable to the situation, and the standard can be met without the specification or alternative, then nothing beyond the standard needs to be put in place.

In all cases the covered entity must document how it is meeting the standards and implementation specifications. The rationale for the selection of an alternative safeguard, or to not implement anything at all, must be documented with particular thoroughness.

See also:
45 CFR 164.306



hipaamail@tma.osd.mil ♦ www.tricare.osd.mil/tmaprivacy